REMARKS

Claims 1-3, 7-12, 15-19, and 21-27 remain pending in the instant application. Claims 1-3, 7-12, 15-19, and 21-23 are allowed. Claims 24-26 presently stand rejected. Claim 27 stands as objected to. Reconsideration of the pending claims are respectfully requested. Applicants thank the Examiner for the indication of the allowed claims.

Claim Rejections – 35 U.S.C. § 102

Claims 24-26 stand rejected under 35 U.S.C. § 102(a) as being anticipated by Garfinkel et al., "Terra: A Virtual Machine-Based Platform for Trusted Computing," ACM, 2003. Applicants respectfully traverse the rejections.

A claim is anticipated only if each and every element of the claim is found in a single reference. M.P.E.P § 2131 (citing *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628 (Fed. Cir. 1987)). "The identical invention must be shown in as complete detail as is contained in the claim." M.P.E.P. § 2131 (citing *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226 (Fed. Cir. 1989)).

Independent claim 24 recites:

A method, comprising:

loading an untrusted virtual machine monitor (VMM) to support a plurality of virtual machines in a computer system, the VMM including a VMM multiplexer;

loading a first and a second virtual machine (VM) supported by the VMM;

sharing a trusted hardware device between the first VM and the second VM using the VMM multiplexer;

receiving a request for a VMM service that is associated with the first VM, wherein the request comprises a challenger hash value;

computing a current compound hash value based on a combination of the first VM platform configuration including the challenger hash value and the second VM platform configuration including the second VM hash value;

determining whether the current compound hash value is equal to the stored compound hash value; and

executing the received request when the current compound hash value is equal to the stored compound hash value.

Applicants respectfully submit that *Garfinkel* fails to disclose at least the above limitations. In particular, Applicants note that the cited art fails to compute (and subsequently use) a compound hash value using information from a first and second virtual machine. The Examiner argues that Section 4.2 (page 199) teaches computing a current compound hash value based on a combination of the first VM platform configuration including the challenger hash value and the second VM platform configuration including the second VM hash value. Instead, *Garfinkel* teaches implementing attestation of subsections of a hashed entity (Section 4.2, third paragraph) where "Terra" divides attestable entities (i.e., entire entities) into fixed-size blocks. The VM descriptor contains a hash over those hashes (for the fixed-size blocks). Thus, the hashes are associated with a single VM, and do not include a second VM hash value from a second VM platform configuration.

Accordingly, *Garfinkel* teaches away from a second VM platform configuration including the second VM hash value because *Garfinkel* teaches attestation solely between a single VM and a single remote party (page 195, right column, fifth full paragraph). The attestation is addressed to a particular piece of software (for which the third party already has a hash value, *see* section 4.3, third paragraph) rather than to a hardware configuration, as recited by the claim. Further, "Receiving an attestation tells the remote party what program was started on a platform, but it does not confirm that the program has not subsequently been compromised" (*see*, section 2.2, first paragraph) Thus the hash values of *Garfinkel* are directed toward specific, known-beforehand software applications, rather than verifying known current hardware configurations of VMs.

Garfinkel teaches away from computing a **compound** hash value using information from a first and second virtual machine because the remote parties perform the attestation for a single VM themselves (see above paragraph), and do not teach determining a second VM platform configuration including a second hash value based on information measured from the second VM. The remote parties do not normally have knowledge of other VMs running on the VMM because the purpose of attestation is to enable "an application in a VM to authenticate itself to remote parties" (*see*, section 2.2 first paragraph, which does not involve a secondary VM). As recited, the compound hash relies on information from a first and second VM. As taught in the specification on page 13, lines 11 and 12, "Even if a hacker were to gain access to a single VM, the hacker could not discover the composite hash value." This security feature is not present

with mere attestation because the attestation merely provides a limited level of security for the benefit of the remote party (*see*, section 2.2, first paragraph, last sentence).

Because *Garfinkel* does not teach a compound hash value based on information from a first and second VM (and a subsequently created **current** compound hash value), it does not execute the received request in response to a determination that the current compound hash value (based on information from a first and second VM) is equal to the stored compound hash value.

Consequently, *Garfinkel* fails to disclose each and every element of claim 24, as required under M.P.E.P. § 2131. Accordingly, Applicants request that the instant §102 rejections of claim 24 be withdrawn.

The dependent claims 25, 26, and 27 are novel over the prior art of record for at least the same reasons as discussed above in connection with their respective independent claims, in addition to adding further limitations of their own. Accordingly, Applicants respectfully request that the instant § 102 rejections of the dependent claims be withdrawn.

Claim Objections

Claim 27 stands objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Claim 27 is believed to be allowable for at least the reasons stated above with respect to the base claim.

CONCLUSION

In view of the foregoing remarks, Applicants believe the applicable rejections have been overcome and all claims remaining in the application are presently in condition for allowance. Accordingly, favorable consideration and a Notice of Allowance are earnestly solicited. The Examiner is invited to telephone the undersigned representative at (206) 292-8600 if the Examiner believes that an interview might be useful for any reason.

CHARGE DEPOSIT ACCOUNT

It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a). Any fees required therefore are hereby authorized to be charged to Deposit Account No. 02-2666. Please credit any overpayment to the same deposit account.

Respectfully submitted,
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP

Date: January 22, 2008 /Mark R. Hennings/

Mark R. Hennings
Reg. No. 48,982
Phone: (206) 292-8600

1279 Oakmead Parkway
Sunnyvale, California
94085-4040